Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ’ όλο τον κόσμο...

Δελτίο 174
15 Μάη 2010

India's Electronic Voting Machines Are Vulnerable to Attack
University of Michigan News Service (04/28/10), N. Moore

A University of Michigan (UM) collaborative study has found that India's direct recording electronic (DRE) voting machines are vulnerable to fraud. UM researchers demonstrated two attacks against an Indian electronic voting machine. One attack involves replacing a part with a similar-looking component that can be instructed to steal a percentage of the votes from a candidate. Another attack uses a small device to change the votes stored in the machine. "Almost every component of this system could be attacked to manipulate election results," says UM professor J. Halderman. However, the Election Commission of India claims that weaknesses found in other electronic voting systems around the world do not apply to India's DRE machines, which it called "fully tamper-proof." DREs store votes in internal memory and provide no paper records for later inspection or recount. "Such machines have already been abandoned in Ireland, the Netherlands, Germany, Florida, and many other places," says R. Gonggrijp, a security researcher from the Netherlands who took part in the study. "India should follow suit."

Computer Experts Tackle Privacy, Security Policy Issues at CFP 2010
ACM (04/29/10)

The 20th Annual ACM Computers, Freedom and Privacy (CFP) Conference will address several key issues, including privacy in the cloud, healthcare information technology, social network activism, the 2010 census, and human rights. Microsoft chief privacy strategist P. Cullen will give a keynote address on privacy issues in cloud computing, while human rights in the context of the Web will be the focus of the keynote address of Google chief legal officer D. Drummond. The American Civil Liberties Union of Northern California's N. Ozer will lead the opening panel, entitled "Privacy and Free Speech: It's Good For Business." CFP 2010 also will offer a technology fair; sessions on "Investing in Privacy," "The Internet of Things," and "Foundations of Trust Online;" the first "Unconference on Computers, Freedom and Privacy;" graduate student poster sessions; and birds of a feather roundtable sessions. CFP 2010 will be held June 15-18 at San Jose State University.

Attack Makes Chips More Reliable
BBC News (04/26/10), M. Ward

University of Michigan (UM) researchers have discovered that by varying the voltage to certain parts of a computer's processor, the ability to keep key data secret is compromised. The researchers also found that a method that helps chips defend against the attack also could make them more reliable. "By putting the voltage just below where it should be means the device makes computational mistakes--it suffers temporary transistor failure," says UM professor V. Bertacco. The researchers used that insight to develop an attack method that could extract every part of a 1,024-bit key in about 100 hours. The research will lead to improvements in the way the public key security system works to make it less susceptible to this kind of attack, Bertacco says. The research also could help to produce error correction systems that identify when transistors fail and ensures that the data does not get corrupted.

EU Security Agency Backs Cloud Computing Research
V3.co.uk (04/29/10), P. Muncaster

A report from European Union security agency ENISA says that cloud computing, wireless networks, and supply chain integrity should be the focus of information technology security research during the next three to five years. Europe must focus on policy and law enforcement challenges, in addition to technical issues, according to the report. "Cloud computing models can benefit greatly from the international harmonization of data protection, retention, and privacy regulations," the report says. "Research is also needed to better understand the best practices and policies that will facilitate effective incident handling." The study also calls for guidelines and standards for evaluating and certifying cloud-based services. Real-time detection and diagnosis systems, future wireless networks, and sensor networks are other areas in need of greater attention from researchers. With regard to wireless network security, Europe must address the requirements for resilience, as well as network mechanisms, intrusion detection, and recovery mechanisms.

UK Competition Aims to Find Future Cyber-Security Experts
Tech Watch (UK) (04/29/10), D. Allan

A group of businesses, police, and government organizations in Great Britain have launched the Cyber Security Challenge UK as part of an effort to improve cybersecurity in the country. Challenge participants will take tests on how to defend networks and identify security vulnerabilities in Web site code, among other things, to determine whether they have the skills needed for a career in cybersecurity. Those who pass the tests will then undergo head-to-head challenges. Participants who do well on the challenges may then be eligible to receive training and scholarships so that they can further develop their cybersecurity skills. The launch of the Cyber Security Challenge UK comes in the wake of the release of a report from the House of Lords that found that future wars will increasingly involve cyberattacks. The report also criticized other European nations for not doing enough to boost cybersecurity.

Computer Science Shows How 'Twitter-Bombs' Wield Influence
Wellesley College (05/03/10), A. Corday

Wellesley College computer science professor P. Takis Metaxas says "Twitter bombs"- sending many Tweets from a large number of Twitter accounts within a short period of time - are being used to affect the outcome of elections. Metaxas says Twitter bombs were used against US Senate candidate M. Coakley in the recent Massachusetts senatorial election. A Twitter bomb reaches many people very quickly. "In addition, because Google is displaying Twitter trends in a prominent place, you influence Google search results," Metaxas says. The result of the Twitter bomb was "disproportionate exposure to personal opinions, fabricated content, unverified events, lies, and misrepresentations that would otherwise not find their way in the first page (of Google search results), giving them the opportunity to spread virally," he says. In an analysis of the Coakley Twitter bomb, the researchers found that the attack was launched by the American Future Fund, the same group that attacked J. Kerry's record during his 2004 presidential campaign. Metaxas is developing software to detect Twitter bombs in real time.

Improved Online Security for a Tenth of the Cost
University of Hertfordshire (05/11/10)

Computer scientists in the United Kingdom are developing a system that would offer a high level of security at one-tenth the cost of existing systems that use special quantum technology. The fiber-optics system would offer security to two online users by broadcasting a continuous stream of information around the communication loop. Access to the information would be limited to users who have a secret key. "It is like using background noise to allow two users to share a secret that no one else knows," says University of Hertfordshire professor B. Christianson. The fiber-optics system uses a leak-proof error correction-based protocol to ensure integrity. "Various people have proposed similar ideas in the past, but our system has introduced a novel error correcting scheme, which means we can use cheap fiber-optics technology and make it work at amazingly high transmission rates," Christianson notes.

'Tamper Evident' CPU Warns of Malicious Backdoors
The Register (UK) (05/12/10), D. Goodin

Columbia University scientists have developed a chip design that prevents microprocessors from being equipped with malicious backdoors that could be used to steal sensitive information or receive instructions from adversaries. The researchers' "tamper evident" microprocessor is designed to monitor operations flowing through a CPU for signs that its microcode has been altered during the design cycle. "The root of trust in all software systems rests on microprocessors because all software is executed by a microprocessor," the researchers say. The tamper-evident chip features two engines hardwired into a processor that continuously monitors chip communications for anomalies. One of the engines, called TrustNet, sends an alert whenever a unit executes more or fewer instructions than is expected. The second engine, called DataWatch, watches chip data for signs the CPU has been maliciously modified.

US Struggles to Ward Off Evolving Cyber Threat
Reuters (05/12/10), P. Stewart; J. Wolf

More than 100 foreign spy agencies, as well as criminal organizations and terrorist groups, are probing US computer systems thousands of times per day and scanning them millions of times daily, says US Dept. of Defence official J. Miller. He says authorities have failed to stay ahead of the cyberattacks, which have resulted in the loss of an enormous amount of data. Miller says the problem is compounded by the fact that the US does not fully understand the vulnerabilities that hackers are taking advantage of. However, he says there are several steps the US could take to improve cybersecurity, including working with private industry to protect potential vulnerabilities in vital infrastructure such as power grids and financial markets. Miller also says the US needs to focus on developing more computer programmers, since countries such as China and India are expected to produce many more computer scientists than the US will over the next 20-30 years.